(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 981 115 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
23.02.2000 Patentblatt 2000/08

(51) Int. Cl.[7]: **G07F 7/10**, G06K 19/07, G06F 12/14

(21) Anmeldenummer: **99113007.1**

(22) Anmeldetag: **06.07.1999**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **20.08.1998 DE 19837808**

(71) Anmelder:
Orga Kartensysteme GmbH
33104 Paderborn (DE)

(72) Erfinder:
- **Jahnich, Michael, Dr.**
  33098 Paderborn (DE)
- **Wüppenhorst, Guido**
  33102 Paderborn (DE)
- **Doppmeier, Werner**
  33397 Rietberg (DE)

(54) Verfahren zur Ausführung eines Verschlüsselungsprogramms zur Verschlüsselung von Daten in einem mikroprozessorgestützten, tragbaren Datenträger

(57) Es wird ein Verfahren zur Ausführung eines Verschlüsselungsprogramms zur Verschlüsselung von Daten in einem mikroprozessorgestützten, tragbaren Datenträger beschrieben, wobei das Verschlüsselungsprogramm mehrere parallelisierbare Unterprogramme aufweist. Erfindungsgemäß wird bei der Ausführung des Verschlüsselungsprogramms die zeitliche Ausführungsreihenfolge von mindestens zwei Unterprogrammen unter Berücksichtigung von mindestens einer Zufallszahl zufällig vertauscht.

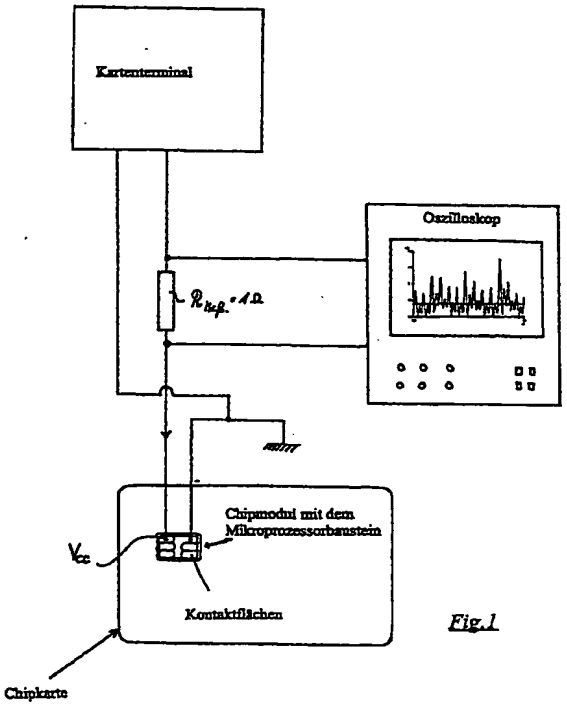

Fig.1

EP 0 981 115 A2

Beschreibung

[0001] Die Erfindung bezieht sich aufein Verfahren zur Ausführung eines Verschlüsselungsprogramms zur Verschlüsselung von Daten in einem mikroprozessorgestützten, tragbaren Datenträger. Ein derartiger tragbarer Datenträger ist beispielsweise eine Chipkarte, die zum Datenaustausch und zur Energieversorgung mit einem entsprechenden Kartenterminal, dem Datenaustauschgerät, verbunden wird. Mikroprozessorchipkarten, die in der Lage sind, anhand eines Verschlüsselungsprogramms Daten zu verschlüsseln, werden beispielsweise in Form von Bankkarten oder in Form von Zugangsberechtigungskarten zu Mobilfunknetzen nach dem GSM-Standard eingesetzt. Der Verschlüsselung von Daten und Informationen kommt dabei eine immer größere Bedeutung zu. Dementsprechend steigen auch die Anforderungen an die Sicherheit der Verschlüsselung gegenüber Angriffen.

[0002] Die tragbaren Datenträger, die Gegenstand der vorliegenden Erfindung sind, verfügen nicht über eine eigene Energieversorgung, beispielsweise in Form einer Batterie oder Solarzelle. Die Energieversorgung des tragbaren Datenträgers erfolgt durch das Datenaustauschgerät, mit dem dann auch die Kommunikation stattfindet. Chipkarten weisen auf der Kartenoberfläche elektrische Kontaktflächen auf, um über korrespondierende Kontakte im Datenaustauschgerät mit diesem kommunizieren zu können. Eine dieser Kontaktflächen ist für die Zuführung der Versorgungsspannung und des Versorgungsstroms vorgesehen. Eine andere Kontaktfläche dient dem Masseanschluß, eine der seriellen, bidirektionalen Datenübertragung vom und zum Datenaustauschgerät, eine der Zuführung eines Taktsignals, eine weitere Kontaktfläche ist für den Empfang eines Reset-Signals vorgesehen.

[0003] Die tragbaren Datenträger, die Gegenstand der Erfindung sind, weisen einen integrierten Halbleiterbaustein auf, in dem ein Mikroprozessor mit einem Festwertspeicher (ROM- Read Only Memory), einem flüchtigen Arbeitsspeicher (RAM- Random Access Memory), in den das Betriebssystem oder zumindest Teile davon abgelegt sind, und einem nichtflüchtigen, änderbaren Speicher (EEPROM - Electrical Erasable Programmable Read Only Memory) auf. Damit stellt der tragbare Datenträger eine Mikrorechnereinheit dar, die jedoch einer externen (von außerhalb des tragbaren Datenträgers) Spannungs- und Stromversorgung Bedarf Der Mikroprozessor bildet die Verarbeitungsschaltungen zur Ausführung von Programmen, insbesondere auch von Verschlüsselungsprogrammen, die im EEPROM-Speicher und/oder ROM-Speicher gespeichert sind. Hier sind ebenfalls geheime Schlüssel von außen nicht zugänglich abgespeichert. Diese Schlüssel dienen der Verschlüsselung der Daten. Da die Verschlüsselungsprogramme (Algorithmen) an sich meistens bekannt sind, liegt die ganze Sicherheit hinsichtlich der Verschlüsselung der Daten bei den geheimen Schlüsseln. Die verschlüsselten Daten sind demnach eine Funktion des Verschlüsselungsprogramms in Abhängigkeit von den unverschlüsselten Daten (Klartext) und wenigstens einem geheimen Schlüssel:

$$D_{encrypt} = S(K_{encrypt}, Daten),$$

wobei S für das Verschlüsselungsprogramm steht, $D_{encrypt}$ für die verschlüsselten Daten steht und $K_{encrypt}$ den geheimen Schlüssel bezeichnet.

[0004] Ein derartiges, allgemein bekanntes Verschlüsselungsprogramm ist beispielsweise der sogenannte DES-Algorithmus. Ein solches Verschlüsselungsprogramm besteht wiederum aus mehreren zeitlich aufeinanderfolgenden Programmebenen (Funktionsblöcken), die ihrerseits wiederum mehrere Unterprogramme aufweisen, wobei die zeitliche Ausführungsreihenfolge von bestimmten Unterprogrammen ohne Einfluß aufdas Ergebnis der Verschlüsselung ist. Man spricht hier von an sich parallelisierbaren Unterprogrammen, die jedoch in dem tragbaren Datenträger sequentiell abgearbeitet werden. Unterprogramme in diesem Sinne können sein : Prozeduren, Routinen und Kommandos.

[0005] Aufgrund des physikalischen Aufbaus und der physikalischen Eigenschaften der in den tragbaren Datenträgem eingesetzten Halbleiterchips ist die Strom- bzw. Leistungsaufnahme des tragbaren Datenträgers während der Ausführung von Programmen nicht konstant, sondern vielmehr zeitlichen Schwankungen unterworfen. Dabei hat es sich gezeigt, daß die Schwankungen des Versorgungsstroms sogar zu bestimmten Programmkommandos und zur binären Struktur (Zahl der Nullen und Einsen) der zu verarbeitenden Daten korreliert. Unter Umständen erfolgen die Schwankungen sogar synchron zum Takt mit dem der tragbare Datenträger betrieben wird. Für einen mit der Technik vertrauten, unbefugten Benutzer ist es ein leichtes diese Schwankungen des Versorgungsstromes, der vom Datenaustauschgerät an den tragbaren Datenträger geliefert wird mittels eines Speicher-Oszilloskops aufzuzeichnen, indem er in die Versorgungsstromleitung einen Meßwiderstand einbaut und den Spannungsabfall an diesem aufdem Oszilloskop aufzeichnet. Mit Blick aufdie Ausführung von Verschlüsselungsprogrammen in tragbaren Datenträger ergibt sich hiermit für Angreifer die Möglichkeit über die Aufzeichnung der Stromschwankungen beim Ausführen des Verschlüsselungsprogramms Rückschlüsse aufdie verwendeten geheimen Schlüssel und/oder die zu verschlüsselten Daten zu ziehen. Dies wird insbesondere dadurch erleichtert, daß die Verschlüsselungsprogramme einschließlich der darin verwendeten Unterprogramme an sich bekannt sind. Zeichnet ein Angreifer nun für eine Vielzahl von Verschlüsselungen mit jeweils unterschiedlichen Daten jeweils die Stromschwankungen auf, so kann er aus Unterschieden in den jeweiligen Stromschwankungs-Charakteristika Rückschlüsse auf

die oder den verwendeten Schlüssel ziehen. Hierbei kann ein Angreifer aufaus der Mathematik bekannte statistische Analysemittel und Korrelationsverfahren zurückgreifen. Hat der Angreifen auf diese Weise den geheimen Schlüssel herausgefunden, so ist Sicherheit der Verschlüsselung nicht mehr gewährleistet, da die Verschlüsselungsprogramme an sich bekannt sind. Insbesondere bei symmetrischen Verschlüsselungsverfahren, wo zur Ver- und Entschlüsselung ein und derselbe Schlüssel verwendet wird, wäre der Angreifer dann in der Lage verschlüsselte Daten zu entschlüsseln.

[0006] Ein derartiger Angriff auf die Sicherheit von tragbaren Datenträgern wird als Differenital Power Analysis (DPA) bezeichnet. Zur Lösung dieses Problems wird in der C2-Intern, Edition Nr. 67, vom 15.7.98 (Kopie ist als Anhang zum Patentantrag beigefügt) vorgeschlagen, in den tragbaren Datenträger eine zusätzliche elektronische Schaltung einzubringen, die die Stromschwankungen kompensieren soll, so daß ein Angreifer diese nicht mehr feststellen kann und daraus Rückschlüsse ziehen kann.

[0007] Diese Lösung ist jedoch sehr aufwendig und teuer, da sie die Implementierung eines zusätzlichen elektronischen Bauteils erfordert. Dajedoch insbesondere der Chipkartenmarkt ein Massenmarkt ist, ist hier der Preisdruck besonders hoch, so daß eine derart aufwendige und teuere Lösung nicht akzeptabel ist.

[0008] Aufgabe der Erfindung ist es daher, tragbare Datenträger der oben genannten Art gegenüber einem Angriff auf die Sicherheit bei der Datenverschlüsselung in effektiver, einfacher und kostengünstiger Weise sicherer zu machen.

[0009] Diese Aufgabe wird durch die Merkmale des Patentanspruchs 1 gelöst. Die sich daran anschließenden Unteransprüche enthalten vorteilhafte Ausgestaltungen der Erfindung.

[0010] Erfindungsgemäß wird bei der Ausführung von Verschlüsselungsprogrammen, die aus mehreren Unterprogrammen bestehen, so verfahren, daß die zeitliche Ausführungsreihenfolge von mindestens zwei parallelisierbaren Unterprogrammen unter Berücksichtigung von mindestens einer Zufallszahl bei jeder Programmausführung zufällig vertauscht wird. Parallelisierbare Unterprogramme bei DES-Verschlüsselungsprogrammen sind beispielsweise die dem Fachmann bekannten, sogenannten S-Boxen.

[0011] Durch diese erfindungsgemäße Verfahrensweise werden zufällig in für einen Angreifer nicht vorhersehbarer Weise Stromschwankungen erzeugt, die es ihm erheblich erschweren oder gar unmöglich machen, anhand der aufgezeichneten Stromschwankungen Rückschlüsse auf den geheimen Schlüssel oder die zu verschlüsselnden Daten zu ziehen. Je größer die Zahl der zufällig vertauschten (permutierten) Unterprogramme, desto „chaotischer" sind die Stromschwankungen und desto schwieriger ist es für einen Angreifer, geheime Daten mittels einer mathematischen Analyse der Stromschwankungen auszuspionieren.

[0012] Das erfindungsgemäße Verfahren läßt sich in einfacher und kostengünstiger Weise programmtechnisch (softwaremäßig) in den tragbaren Datenträger implementieren. Zusätzliche elektronische Bausteine sind nicht notwendig.

[0013] Anhand der beigefügten Zeichnungen soll die Erfindung nachfolgend näher erläutert werden. Es zeigt:

- Fig.1 eine Versuchsanordnung zur Aufzeichnung von Stromschwankungen bei der Ausführung von Verschlüsselungsprogrammen,
- Fig.2 ein Beispiel für den zeitlichen Verlauf des Versorgungsstroms während der Ausführung eines Verschlüsselungsprogramms,
- Fig.3 ein schematisches Strukturgramm eines Verschlüsselungsprogramms,
- Fig.4 den fixen Programmdurchlauf bei der Ausführung eines Verschlüsselungsprogramms nach dem Stand der Technik,
- Fig.5 ein schematisches Strukturgramm eines Verschlüsselungsprogramms, das um Attrappen-Unterprogramme (gestrichelt eingezeichnet) ergänzt wurde,
- Fig.6 eine Tabelle mit den Startadressen von parallelisierbaren Unterprogrammen,
- Fig.7 die Vertauschung von Startadressen mittels Zufallszahlen und die dementsprechend geänderte Bearbeitungsreihenfolge der Unterprogramme.

[0014] In Figur 1 ist ein tragbarer Datenträger in Form einer Mikroprozessor-Chipkarte gezeigt. Der integrierte Halbleiterbaustein mit dem Mikroprozessor und den Speichern (RAM, ROM, EEPROM) befindet sich in einem Chipmodul, das als separates Bauteil in den Kartenkörper eingesetzt wird. Aufdem Chipmodul befinden sich die elektrischen Kontaktflächen zum Datenaustausch und zur Energieversorgung in Verbindung mit dem Datenaustauschgerät (in dem dargestellten Fall ist dies ein Kartenterminal). Aus Gründen der Übersichtlichkeit ist nur die Strom- und Spannungsversorgungsleitung vom Kartenterminal an die entsprechende Kontaktfläche der Karte sowie die Masseleitung eingezeichnet. Für den vorstehend beschriebenen DPA-Angriff auf die Chipkarte, wird in die Stromversorgungsleitung ein Meßwiderstand (z.B. ein 1 Ω) eingebaut und über den Spannungsabfall an diesem Widerstand indirekt die Stromschwankungen gemessen und an einem Speicheroszilloskop aufgezeichnet.

[0015] Wie man in Fig. 2 erkennen kann sind die Stromschwankungsamplituden, die während der Ausführung eines Verschlüsselungsprogramms auftreten können, stellenweise ein Vielfaches der mittleren Stromaufnahme (Gleichstromanteil). Ein Angreifer könnte nun das Verschlüsselungsprogramm in der Chipkarte mehrfach ausführen lassen und dabei jeweils die Stromschwankungen aufzeichnen und mittels mathematischer Analysemethoden versuchen, heraus-

zufinden, ob es Korrelationen zwischen den einzelnen Aufzeichnungen gibt. Zum Beispiel könnte er versuchen herauszufinden, ob bei den verschiedenen Ausführungen des Verschlüsselungsprogamms jeweils an einem bestimmten Zeitpunkt (Zeitabschnitt) gleiche Stromschwankungen aufgetreten sind, die charakteristisch sind für die Verarbeitung von Daten (Daten in diesem Sinne sind auch geheime Schlüssel) mit einer bestimmen Bitmusterstruktur und/oder charakteristisch für die Ausführung von bestimmten Befehlen. Kennt der Angreifer das Verschlüsselungsprogramm und weiß, an welchen Stellen im Programmablauf normalerweise bspw. Schlüssel verarbeitet werden oder bestimmte Befehle ausgeführt werden, so kann er damit an sich geheime Schlüssel ausspionieren.

[0016] In Figur 3 ist ein schematisches Strukturgramm eines Verschlüsselungsprogramms (S) dargestellt. Ein solches Programm besteht aus verschiedenen, zeitlich aufeinanderfolgenden Programmebenen (1 bis m). Innerhalb dieser Programmebenen gibt es wiederum verschiedene Unterprogramme, von denen zumindest einige parallelisierbar sind, d.h. die Reihenfolge in der diese Programme zeitlich hintereinander ausgeführt werden ist unerheblich.. Nach dem Stand der Technik wurde die zeitliche Ausführungsreihenfolge dieser parallelisierbaren Unterprogramme jedoch einmal vom Programmierer festgelegt, was zur Folge hat, daß der Programmdurchlauf durch das Verschlüsselungsprogramm mit seinen Unterprogrammen immer der gleiche ist. Selbst wenn ein Angreifer die Ausführungsreihenfolge der an sich parallelisierbaren Unterprogramme zunächst nicht kennt, so kann er sie durch einen DPA-Angriff doch herausfinden, wenn er das Verschlüsselungsprogramm nur hinreichend oft durchlaufen läßt und jeweils die Stromschwankungen aufzeichnet. Da das Verschlüsselungsprogramm immer gleich durchlaufen wird, lassen sich mit Hilfe mathematischer Methoden Korrelationen zwischen den einzelnen Stromschwankungsaufzeichnungen finden, die Rückschlüsse auf den Programmablauf und darüber hinaus auf geheime Schlüssel gestatten.

[0017] Dadurch, daß der Programmablauf erfindungsgemäß jeweils durch zufällige Vertauschung von parallelisierbaren Unterprogrammen ein anderer ist, lassen sich derartige Korrelationen von einem Angreifer nicht mehr oder nur noch mit einem unverhältnismäßig hohen Aufwand herausfinden. Das Ausspionieren von geheimen Schlüsseln wird somit wirksam verhindert oder zumindest erheblich erschwert.

[0018] Die zur zufälligen Vertauschung der Unterprogramme verwendeten Zufallszahlen werden vorzugsweise in einem Zufallszahlengenerator des Chipkarte erzeugt. Ein solcher Zufallszahlengenerator kann beispielsweise in Form eines Softwareprogramms in der Chipkarte implementiert sein. Derartige Programme sind dem Fachmann bekannt. Ferner kann der Zufallszahlengenerator auch eine elektronische Schaltung im tragbaren Datenträger sein (Hardwarevariante). Alternativ zur Erzeugung einer Zufallszahl in der Chipkarte, kann die Zufallszahl auch von dem Kartenterminal an die Chipkarte übermittelt werden.

[0019] Bei einem Verschlüsselungsprogramm, das mehrere bei der Programmausführung zeitlich aufeinanderfolgende Programmebenen mit jeweils mehreren parallelisierbaren Unterprogrammen aufweist, sind für das erfindungsgemäße Verfahren zwei Ausführungsvarianten vorgesehen.

[0020] In der ersten Ausführungsvariante wird jeweils vor Beginn des eigentlichen Verschlüsselungsprogramms die zeitliche Ausführungsreihenfolge für die Ausführung der Unterprogramme auf allen Programmebenen unter Berücksichtigung der Zufallszahl(en) festgelegt. Dabei kann es durchaus so sein, daß nicht notwendiger Weise alle parallelisierbaren Unterprogramme zufällig vertauscht werden, d.h. es kann auch Programmebenen mit parallelisierbaren Unterprogrammen geben, auf denen keine zufällige Vertauschung stattfindet, so daß die Unterprogramme dieser Programmebene bei jedem Programmdurchlauf immer in derselben Reihenfolge ausgeführt werden.

[0021] In der zweiten Ausführungsvariante steht die Ausführungsreihenfolge aller Unterprogramme aufallen Programmebenen nicht schonjeweils vor dem Start des eigentlichen Verschlüsselungsprogramms fest. Hier wird jeweils erst vor dem Eintritt in eine neue Programmebene die zeitliche Ausführungsreihenfolge für die Unterprogramme auf dieser Programmebene unter Berücksichtigung einer Zufallszahl(en) bestimmt.

[0022] Zur Realisierung der Vertauschung der Ausführungsreihenfolge von parallelisierbaren Unterprogrammen wird vorzugsweise mit einer Tabelle gearbeitet, in der die Programmstartadressen der parallelisierbaren Unterprogramme hinsichtlich ihrer Reihenfolge-Position gespeichert sind -vgl. Fig.6. Diese Tabelle wird vorzugsweise im RAM-Speicher der Chipkarte programmäßig erzeugt. Die Einträge in diese Tabelle werden nun - wie weiter unten erläutert wird - erfindungsgemäß zufällig vertauscht.

[0023] Die Programmstartadressen sind ferner im nichtflüchtigen EEPROM-Speicher der Chipkarte gespeichert. Vor dem Start des eigentlichen Verschlüsselungsprogramms werden die Programmstartadressen der Unterprogramme nacheinander aus dem EEPROM und/oder ROM-Speicher geladen und ins RAM geschrieben. Damit wird die Tabelle gewissermaßen auf Anfangswerte gesetzt. Nun wird ein Zufallszahlen-Paar bestehend aus zwei Zufallszahlen (Z1, Z2) erzeugt, dabei entspricht die Menge der möglichen Zufallszahlen der Menge der Reihenfolge-Positionen - vgl. Fig.7. Enthält das Verschlüsselungsprogramm beispielsweise 4 parallelisierbare Unterprogramme, so existieren auch 4 Reihenfolge-Positionen (1,2,3,4), die bestimmen, in welcher Reihenfolge diese ausgeführt werden. Dementsprechend gibt es auch 4 mögliche Zufallszahlen (1,2,3,4). Wird nun das Zufallszahlen-Paar Z1 = 2/Z = 4 generiert, so wird mittels eines ent-

sprechenden Programms die Startadresse des 4. Unterprogramms auf die Reihenfolge-Position 2 geschrieben und die Startadresse des 2. Unterprogramms auf die Reihenfolge-Position 4.

[0024] Durch die erneute Generierung eines Zufallszahlen-Paares und demgemäßes erneutes Vertauschen wird die Ausführungsreihenfolge gegenüber der Anfangseinstellung weiter „durcheinandergewürfelt". Lautet das zweite Zufallszahlen-Paar bspw. (4,3) so wird die Startadresse des 2. Unterprogramms auf die Reihenfolge-Position 3 geschrieben und die Startadresse des 3. Unterprogramms auf die Reihenfolge-Position 4.

[0025] Die Reihenfolge, in der die Unterprogramme nun innerhalb des Verschlüsselungsprogramms ausgeführt werden, ist dann:

1 .Unterprogramm(S1)/ 4.Unterprogramm (S4)/2.Unterprogramm (S2)/3. Unterprogramm (S3).

[0026] In Fig. 5 ist ein schematisches Strukturgramm eines Verschlüsselungsprogramms bestehend aus mehreren Programmebenen gezeigt, wobei dieses aufbestimmten Programmebenen um sogenannte „Attrappen-Unterprogramme" erweitert wurde. Diese „Attrappen-Unterprogamme" sind eigentlich nicht Bestandteil des Verschlüsselungsprogramms. Ihre Ausführung hat somit auch keinen Einfluß auf das Verschlüsselungsergebnis. Allerdings bewirkt ihre Ausführung in vorteilhafter Weise zusätzliche, bei einer DPA-Analyse zu beobachtende Stromschwankungen und tragen somit zu einer weiteren Verwirrung eines Angreifers bei. „Attrappen-Unterprogamme" in diesem Sinne sind wiederum: Prozeduren, Routinen und Kommandos, deren Ausführung allerdings keinen Einfluß auf die Verschlüsselung an sich hat. In diesem Sinne sind sie programmtechnischer Ballast, der sich jedoch vorteilhaft gegenüber einem DPA-Angriff verwenden läßt, insbesondere dann, wenn auch diese „Attrappen-Unterprogramme" erfindungsgemäß zufällig mitvertauscht werden. Durch die Implementierung von „Attrappen-Unterprogrammen" und deren zufällige Vertauschung werden nicht nur zusätzliche Stromschwankungen erzeugt, die nichts mit dem Verschlüsselungsprogramm an sich zu tun haben, sondern sie tauchen auch noch zeitlich zufällig verteilt auf, wodurch ein DPA-Angriffweiter erschwert wird. Darüber hinaus ist es vorgesehen, das die Ausführung bestimmter „Attrappen-Unterprogramme" unter Berücksichtigung mindestens einer Zufallszahl zufällig ausbleiben kann, wodurch weitere Verwirrung für einen DPA-Angreifer geschaffen wird.

[0027] Bei der erfindungsgemäßen Implementierung des Verschlüsselungsprogramms könnte bspw. jede Programmebene um eine solche Zahl von „Attrappen-Unterprogramme" erweitert werden, daß die Zahl der Unterprogramme pro Programmebene insgesamt gleich ist.

[0028] Das erfindungsgemäße Verfahren ist nicht auf sogennate kontaktbehaftete tragbare Datenträger beschränkt. Vielmehr ist sie auch auf sogeannte konktaktlos arbeitende tragbare Datenträger beschränkt, bei denen der Datenaustausch und die Energieversorgung mit dem Datenaustauschgerät über elektromagnetische Strahlung (induktiv) erfolgt, da auch hier mit einem gegenüber dem in Fig.1 dargestellten, modifizierten Meßaufbau die Leistungsaufnahme des tragbaren Datenträgers zu ermitteln ist.

[0029] Die Erfindung ist selbstverständlich auch auf die Ausführung von Entschlüsselungsprogrammen anzuwenden und nicht nur auf Verschlüsselungsprogramme, da die oben beschriebene Problematik dieselbe ist. Außerdem ist die Entschlüsselung ja nichts anderes als eine inverse Verschlüsselung und umgekehrt.

Patentansprüche

1. Verfahren zur Ausführung eines Verschlüsselungsprogramms zur Verschlüsselung von Daten in einem mikroprozessorgestützten, tragbaren Datenträger, der zum Datenaustausch und zur Energieversorgung mit einem Datenaustauschgerät verbunden wird, wobei das Verschlüsselungsprogramm mehrere parallelisierbare Unterprogramme (Routinen, Prozeduren, Kommandos) aufweist, dadurch gekennzeichnet, daß bei der Ausführung des Verschlüsselungsprogramms die zeitliche Ausführungsabfolge von mindestens zwei Unterprogrammen unter Berücksichtigung von mindestens einer Zufallszahl bei jeder Programmausführung zufällig vertauscht werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Zufallszahl in einem Zufallszahlengenerator des tragbaren Datenträgers erzeugt wird.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß der Zufallszahlengenerator als Programm in dem tragbaren Datenträger implementiert ist.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Zufallszahl von dem Datenaustauschgerät an den tragbaren Datenträger übermittelt wird.

5. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß bei einem Verschlüsselungsprogramm, das mehrere bei der Programmausführung zeitlich aufeinanderfolgende Programmablaufebenen mitjeweils

mehreren Unterprogrammen aufweist, jeweils vor Beginn der Programmausführung die zeitliche Ausführungsreihenfolge für die Ausführung der Unterprogramme auf allen Programmablaufebenen unter Berücksichtigung von mindestens einer Zufallszahl festgelegt wird.

6. Verfahren nach einem der vorstehenden Ansprüche 1 bis 4,
dadurch gekennzeichnet, daß
bei einem Verschlüsselungsprogramm, das mehrere bei der Programmausführung zeitlich aufeinanderfogende Programmablaufebenen mit jeweils mehreren Unterprogrammen aufweist, jeweils vor Beginn der Programmausführung die zeitliche Ausführungsreihenfolge für die Ausführung der Unterprogramme auf nur bestimmten Programmablaufebenen unter Berücksichtigung von mindestens einer Zufallszahl festgelegt wird.

7. Verfahren nach einem der vorstehenden Ansprüche 1 bis 4,
dadurch gekennzeichnet, daß
bei einem Verschlüsselungsprogramm, das mehrere bei der Programmausführung zeitlich aufeinanderfogende Programmablaufebenen mit jeweils mehreren Unterprogrammen aufweist, jeweils vor dem Eintritt in eine neue Programmablaufebene die zeitliche Ausführungsreihenfolge für die Ausführung der Unterprogrammne auf dieser Programmablaufebene unter Berücksichtigung von mindestens einer Zufallszahl festgelegt wird.

8. Verfahren nach einem der vorstehenden Ansprüche,
dadurch gekennzeichnet, daß

- in dem tragbaren Datenträger eine Tabelle vorgesehen ist, in der die Ausführungsreihenfolge der Unterprogramme anhand von Reihenfolge-Positionen gespeichert ist,
- ein Zufallszahlen-Paar bestehend aus zwei Zufallszahlen ermittelt wird, wobei die Menge der möglichen Zufallszahlen der Menge der Reihenfolge-Positionen entspricht,
- die Reihenfolge-Positionen der Unterprogramme entsprechend des Zufallszahlen-Paares vertauscht wird, wobei die Reihenfolge-Position eines Unterprogramms entsprechend der einen Zufallszahl gegen die Reihenfolge-Position eines anderen Unterprogramms entsprechend der zweiten Zufallszahl ausgetauscht wird.

9. Verfahren nach Anspruch 8,
dadurch gekennzeichnet, daß das Verfahren nach Anspruch 8 zwei- oder mehrfach angewendet wird.

10. Verfahren nach einem der vorstehenden Ansprüche,
dadurch gekennzeichnet, daß
das Verschlüsselungsprogramm um mindestens ein eigentlich nicht zum Verschlüsselungsprogramm gehörendes Attrappen-Unterprogramm erweitert wird, dessen Ausführungsreihenfolgejeweils unter Berücksichtigung von mindestens einer Zufallszahl mitvertauscht wird.

11. Verfahren nach Anspruch 10,
dadurch gekennzeichnet, daß
bei der Ausführung des Verschlüsselungsprogramm jeweils unter Berücksichtigung von mindestens einer Zufallszahl die Ausführung bestimmter Attrappen-Unterprogramme ausbleibt.

12. Verfahren nach einem der Ansprüche 10 oder 11,
dadurch gekennzeichnet, daß
jede Programmablaufebene um Attrappen-Unterprogramme erweitert wird, so daß die Zahl der Unterprogramme pro Programmablaufebene gleich ist.

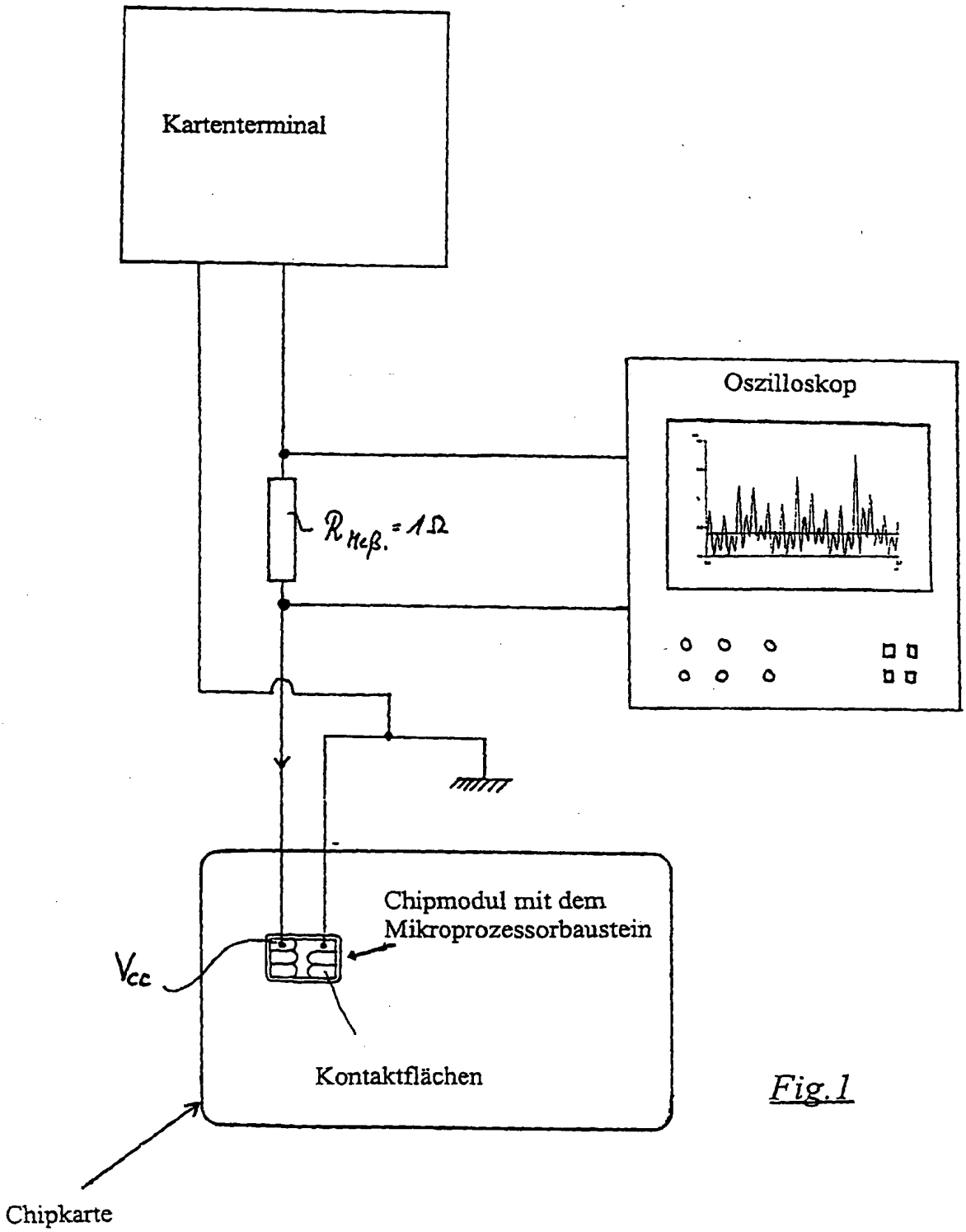
Kartenterminal
Oszilloskop
$R_{Meß.} = 1\,\Omega$
Chipmodul mit dem
Mikroprozessorbaustein
V_{cc}
Kontaktflächen
Chipkarte

Fig.1

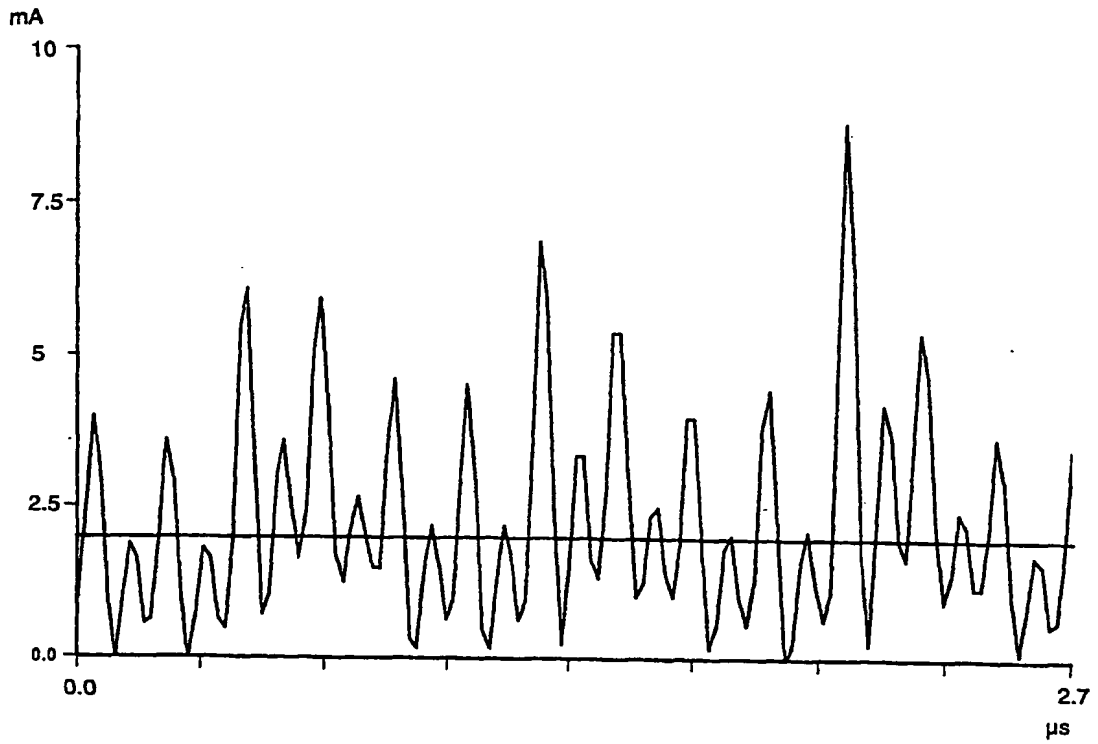

Fig.2

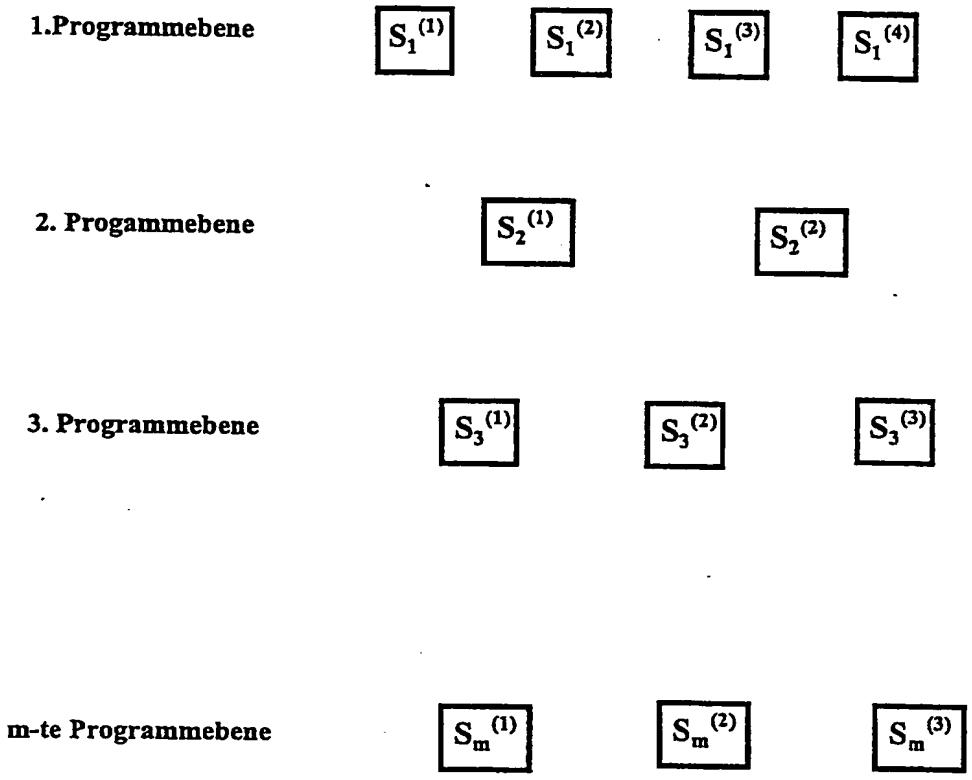
1.Programmebene
$S_1^{(1)}$
$S_1^{(2)}$
$S_1^{(3)}$
$S_1^{(4)}$
2. Progammebene
$S_2^{(1)}$
$S_2^{(2)}$
3. Programmebene
$S_3^{(1)}$
$S_3^{(2)}$
$S_3^{(3)}$
m-te Programmebene
$S_m^{(1)}$
$S_m^{(2)}$
$S_m^{(3)}$

Fig.3

THIS PAGE BLANK (USPTO)

Programmdurchlauf nach dem Stand der Technik

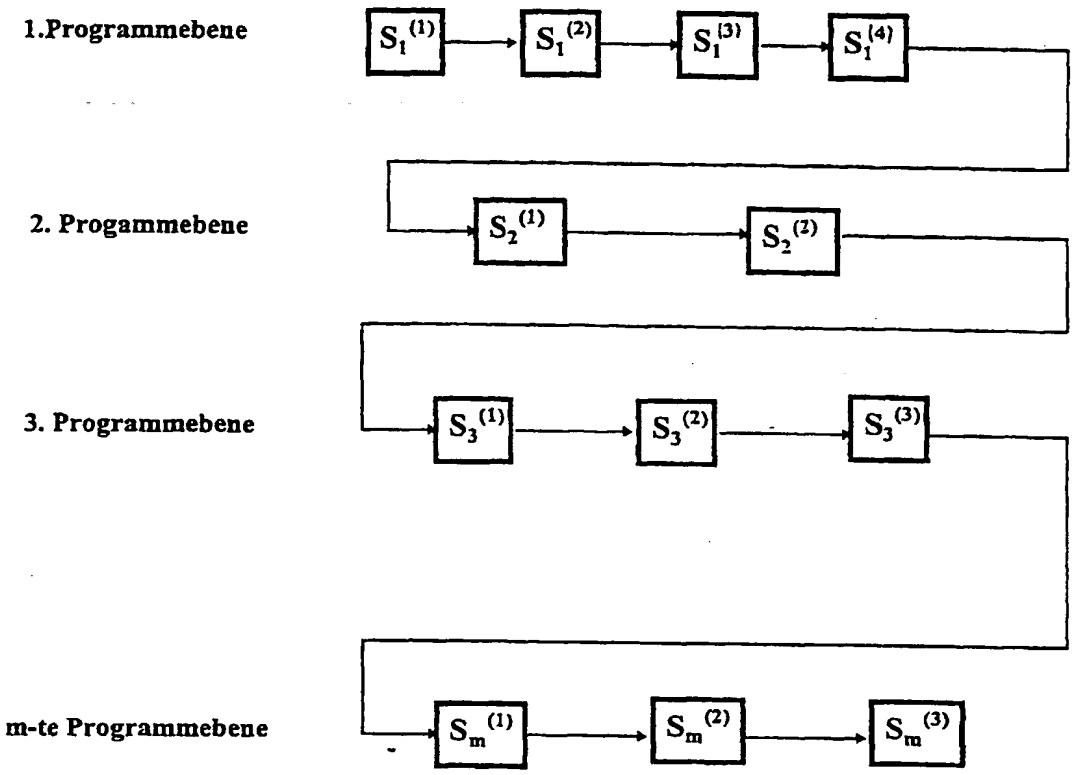

Fig.4

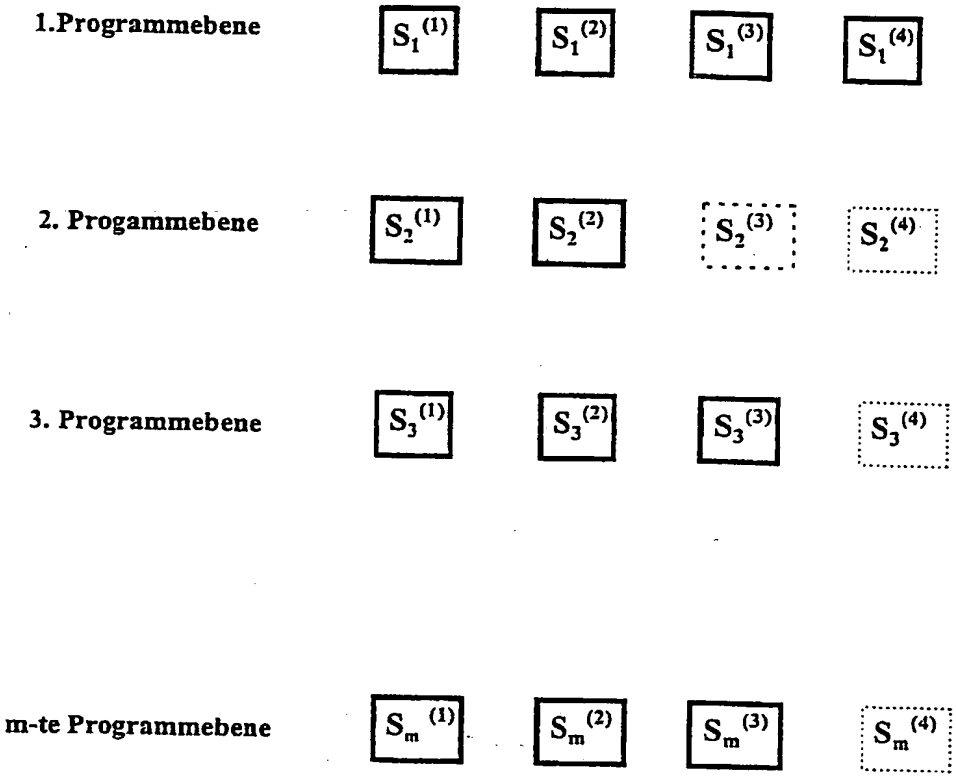
1.Programmebene
$S_1^{(1)}$
$S_1^{(2)}$
$S_1^{(3)}$
$S_1^{(4)}$
2. Progammebene
$S_2^{(1)}$
$S_2^{(2)}$
$S_2^{(3)}$
$S_2^{(4)}$
3. Programmebene
$S_3^{(1)}$
$S_3^{(2)}$
$S_3^{(3)}$
$S_3^{(4)}$
m-te Programmebene
$S_m^{(1)}$
$S_m^{(2)}$
$S_m^{(3)}$
$S_m^{(4)}$

Fig.5

Tabelle mit den Startadressen von parallelisierbaren Unterprogrammen

1. Startadresse des Unterprogramms, das als erstes auszuführen ist: z.B. S1
2. Startadresse des Unterprogramms, das als zweites auszuführen ist: z.B. S2
3. Startadresse des Unterprogramms, das als drittes auszuführen ist: z.B. S3
4. Startadresse des Unterprogramm, das als viertes auszuführen ist: z.B. S4

Fig.6

Fig.7

Vertausch von Startadressen anhand von Zufallszahlen

Ermittlung eines Zufallszahlen-Paares (Z1, Z2) anhand eines Zufallszahlengenerators

Beispiel: Z1 = 2
Z2 = 4

⇨ Startadresse in der 2.Zeile der Startadressen-Tabelle wird gegen die Startadresse in der 4. Zeile ausgestauscht

⇨ neue Startadressen-Tabelle

1.	Startadresse von Unterprogramm S1
2.	Startadresse von Unterprogramm S4
3.	Startadresse von Unterprogramm S3
4.	Startadresse von Unterprogramm S2

Erneute Ermittlung eines Zufallszahlen-Paares

Beispiel: Z1 = 4
Z2 = 3

⇨ Startadresse in der 4. Zeile der Startadressen-Tabelle wird gegen die Startadresse in der 3. Zeile ausgestauscht

⇨ neue Startadressen-Tabelle

1.	Startadresse von Unterprogramm S1
2.	Startadresse von Unterprogramm S4
3.	Startadresse von Unterprogramm S2
4.	Startadresse von Unterprogramm S3

Hinsichtlich der Bearbeitungsreihenfolge von Unterprogrammen permutierter Programmablauf